UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNTS: 1) SANELSS@GMAIL.COM AND 2) SSBIHSSS@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC AND GOOGLE PAYMENT CORPORATION.

Case No. 4:23-MJ-6256 PLC

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 U.S.C. § 2251 (sexual exploitation of children) and 18 U.S.C. § 2252A (distribution, receipt, and/or possession of child pornography)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Nicholas W Zotos

Applicant's signature

Nicholas Zotos, Special Agent

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 09/22/2023

Patricia L. Cohen

Judge's signature

City and state: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge

Printed name and title

AUSA: Nathan Chapman

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNTS 1) **SANELSS@GMAIL.COM** AND 2) **SSBIHSSS@GMAIL.COM** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC AND GOOGLE PAYMENT CORPORATION.	No. 4:23-MJ-6256 PLC SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Zotos, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and have been since

November 2017. I am currently assigned to the HSI office in Saint Louis, Missouri and am affiliated with the Missouri Internet Crimes Against Children Task Force. I investigate federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I completed training on these and related topics through the Federal Law Enforcement Training Center (FLETC), the National Criminal Justice Training Center, the National Law Enforcement Training on Child Exploitation, and through various in-service trainings offered through my agency and external partners. That training includes the requirement to observe, review, and classify numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in several forms of electronic media. I am a graduate of the Treasury Computer Forensic Training Program's Basic Computer Evidence Recovery Training and Basic Mobile Device Forensics courses. I hold an A+ certification from the Computing Technology Industry Association. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

3. The facts in this affidavit come from personal observations, training and experience, and information obtained from other law enforcement and witnesses. This affidavit is merely intended to show sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (sexual exploitation of children) and 18 U.S.C. § 2252A (distribution, receipt, and/or possession of child pornography), were committed by Sanel SMAJLOVIC. There is also probable cause to search the information

described in Attachment A for evidence, instrumentalities, and contraband of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

LOCATION TO BE SEARCHED

7. The location to be searched is Google Account: sanelss@gmail.com (hereinafter referred to as "SUBJECT ACCOUNT 1"), and Google Account: ssbihsss@gmail.com (hereinafter referred to as "SUBJECT ACCOUNT 2") located at a premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

BACKGROUND CONCERNING EMAIL

8. In my training and experience, I have learned that the Provider provides a variety of on-line services, including electronic mail ("email") access, to the public. The Provider allows subscribers to obtain email accounts at the domain name gmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications

(including retrieved and unretrieved email for the Provider subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the

Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP

addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

13. In general, an email that is sent to the Provider is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

BACKGROUND CONCERNING GOOGLE[1]

14. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

9. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

10. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

11. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

a. Gmail - Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google.

b. Contacts - Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a

time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account, so it is stored in Google Contacts. Google preserves contacts indefinitely unless the user deletes them.

c. Calendar - Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar so it is stored in Google Calendar. Google preserves appointments indefinitely unless the user deletes them.

d. Messaging - Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

e. Google Drive and Keep - Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of

documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them.

f. Photos - Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely unless the user deletes them.

g. Maps - Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-

turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

h. Location history - Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity.

Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

i. Google Pay and records of payments for Google services - A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and- mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

j. Chrome and My Activity - Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by

Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts into automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

k. Google Voice - Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

l. YouTube - Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube

also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

12. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

13. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

14. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was

created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

15. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

16. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, by comparing Google service login history, with location history, to the dates and times that payments were made to known sellers of child pornography, the United States can more definitively link a specific person to those transactions versus any person who may have access to the account.

17. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. For example, reviewing email messages from PayPal or cloud service providers can confirm deliberate actions of a specific person as it relates to those non-Google services. PayPal would likely send transaction confirmation messages which would alert a user if someone used the PayPal account without that user's authorization.

18. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

19. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan

to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

20. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

PROBABLE CAUSE

21. The investigation, described more fully below, involves individuals who have engaged in the sexual exploitation of children through an internet-based, videoconferencing and chat application known as Skype. Based on the investigation, there is probable cause to believe that the user of the SUBJECT ACCOUNTS has engaged or attempted to engage in the sexual exploitation of minors in violation of federal criminal statutes, and that evidence of that conduct will be found within the contents of those accounts.

Background on Online Child Sex Trafficking and Exploitation via Webcam and the Internet

22. HSI is investigating individuals who provide access to pre-produced child sexual abuse material, and live-streaming online webcam shows involving the sexual abuse of children to paying customers worldwide. This growing transnational child-sexual-abuse industry includes child sex traffickers in, among other places, the Philippines, who collect viewership fees from vetted customers scattered throughout the world. Paying customers often request that these child

sex traffickers provide pre-recorded depictions of minors engaging in sexually explicit conduct, or sexually abuse minors in real time during private webcam interactions on a variety of streaming video services and applications, including Skype.

23. Based on my training, experience, and information conveyed to me by other law enforcement agents involved in the investigation of live-streaming depictions of child sexual abuse, I know that it is common for such traffickers in the Philippines and elsewhere to be communicating with a large number of individuals who are paying for access to such material. I also know that it is common for the paying customers to be communicating with other traffickers—and sometimes many other traffickers—who are selling access to similar material over the internet. These individuals often use a variety of money service businesses to pay the traffickers or associates of the traffickers for access to this material, including Western Union, WorldRemit, MoneyGram, PayPal, Xoom, and Remitly. In many instances, customers and traffickers must change payment platforms or create multiple accounts on the same platform using slightly changed identifying information to outpace the efforts of payment platforms in detecting suspicious activity and suspending or disabling accounts deemed as engaging in suspicious transactions.

24. I also know that the purchasing individuals often find ways to capture the live-streamed child sexual abuse and exploitation, either by recording the live shows onto their computers or taking still photographs (including "screen captures" or "screen shots") of the abuse, which can also be stored on the individual's computer or an electronic storage device. Such individuals often also save any pre-produced child sexual abuse material the traffickers provide to their computer or an electronic device for later viewing or distribution.

25. In February of 2023, your affiant received reports from HSI Portland. Based on your affiant's review of the reports, I learned the following:

a. HSI identified an individual (hereinafter referred to as the "TRAFFICKER") operating a child-sex-trafficking network from the Philippines. Based on undercover activity and other investigation, HSI learned that the TRAFFICKER did, in fact, have access to minors to sexually abuse on camera and has offered to provide access, through the TRAFFICKER's Skype account, to visual depictions of one or more minors engaging in sexually explicit conduct in exchange for money.

b. On March 25, 2022, the United States District Court of Maine issued federal search warrant (2:22-MJ-50-JAW) for records pertaining to the Skype account used by the TRAFFICKER. In response, Microsoft provided HSI with information associated with that account on May 13, 2022, and provided additional records on June 8, 2022. The information provided by Microsoft revealed incriminating chat content between the TRAFFICKER and Skype account "xflinkx." Subsequent summons to Microsoft revealed Skype account "xflinkx" lists otaku_sanel@sbcglobal.net as the current email address associated with that account. Your affiant personally reviewed the portion of the search warrant response which included account "xflinkx" and personally reviewed the summons response related to that account.

26. Between March 3, 2023, and September 18, 2023, your affiant obtained and served 25 Department of Homeland Security (DHS) summons requesting information from various electronic service providers, money services businesses, and other entities to ascertain information pertaining to the Skype username "xflinkx," the otaku_sanel@sbcglotal.net email address, and their user. Based on the responses to DHS summons, your affiant reviewed records from Yahoo, Inc., PayPal Inc., Microsoft, Xoom, Moneygram, WorldRemit Corp, Google, T-Mobile, and Charter Communications.

27. Your affiant reviewed the available IP connection history for the "xflinkx" Skype account provided by Microsoft and found an IP address capture associated with the account's "Last Modified Date and Time" on August 31, 2019. I then queried that IP address with Charter Communications who provided records showing the subscriber using that IP address at the time as Brana Smajlovic with both billing and service address listed as 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129, and with phone number as 314-255-6957.

28. Based on your affiant's review of records from T-Mobile, phone number 314-255-6957 is registered to Sanel SMAJLOVIC with service address as 6942 Colonial Woods Drive, Apt 70, Saint Louis, MO, 63129.

29. Based on your affiant's review of records from Yahoo, Inc., I learned that a user created email address otaku_sanel@sbcglobal.net on October 5, 2006, and provided initials "SS" in the field asking for first and last name.

30. Your affiant reviewed records from PayPal Inc, for all accounts associated with the otaku_sanel@sbcglobal.net email address and learned there are a total of 10 active or inactive accounts which used that email address. Seven of those accounts are in the name of Sanel SMAJLOVIC who is 33 years old and resides at 6942 Colonial Woods Dr., Apt 70, Saint Louis County, Missouri. Two other accounts are in the name of Halid Smajlovic, who is 65 years old, and use the same Colonial Woods address on the account. The final account, which is inactive, uses the same Colonial Woods address and is in the name of Brana Smajlovic, who is 58 years old. The Halid or Brana Smajlovic accounts do not have transaction history within the last five years. Seven out of the ten accounts, including the two accounts in the name Halid Smajlovic, list phone number 314-255-6957 subscribed to Sanel SMAJLOVIC. Two more accounts in the name of Sanel SMAJLOVIC do not list phone number at all.

31. On April 12, 2023, your affiant applied for and was granted a search warrant (4:23-MJ-8078 SRW) for records pertaining to Skype account "xflinkx," held by Microsoft Corporation. Microsoft responded to that warrant on July 10, 2023, and your affiant has/continues to review the records. The response from Microsoft included over 58,000 lines of chat between "xflinkx" and 722 unique usernames, between April 20, 2017, and September 14, 2022. Your affiant's review of that material is ongoing but revealed numerous examples of the user of "xflinkx" soliciting or negotiating for, and in many instances seemingly completing, online live video sex shows involving minor females in the Philippines as young as one year old. The chat logs were explicit enough to make clear "xflinkx" was knowingly paying for and directing sex acts be performed on minors in a live international broadcast. In some instances, the traffickers would send photographs as a sample or advertisement of the minor girls available for "xflinkx" to purchase a show with. Some of these sample images themselves displayed minors engaged in sexually explicit conduct. A more detailed sample of these transactions is contained in paragraph 41 below.

32. Contained within the Microsoft warrant return are several instances where the user of "xflinkx" self-identified himself as Sanel SMAJLOVIC in conjunction with providing payment confirmation details to the traffickers in the Philippines. To be sure, your affiant was able to cross-reference the date, time, payment amount, and recipient information discussed in the sex trafficking chats with financial transactions from Money Service Business accounts directly linked to Sanel SMAJLOVIC and listing his home address as 6942 Colonial Woods Dr Apt 70, Saint Louis, MO.

33. In other conversations, the user of "xflinkx" identified himself as Sanel in a more social context and refenced employment for the Federal Reserve Bank. Your affiant consulted with the Federal Reserve Board Office of Inspector General (OIG) and confirmed Sanel

SMAJLOVIC is employed by the Federal Reserve Bank of Saint Louis and has been so employed since October 30, 2017. Your affiant viewed a public LinkedIn profile for "Sanel S.", which lists his employment as a Senior Software Engineer for the Federal Reserve Bank of Saint Louis. The OIG also provided your affiant with information from Sanel SMAJLOVIC's personnel file which listed a home address of record, as 6942 Colonial Woods Dr., Apt. 70, St. Louis, MO 63129 and personal contact email address as SUBJECT ACCOUNT 1.

The SUBJECT ACCOUNTS

34. Based on your affiant's review of records from Xoom, SUBJECT ACCOUNT 1 is the listed email address for Sanel SMAJLOVIC's Xoom Account 10821485. Xoom is a PayPal Inc. service that operates as a money service business. That account made 36 payments to the Philippines from May 2018 to September 2019, including at least 12 payments that your affiant cross-referenced to actual sex trafficking shows from the chat log.

35. Based on your affiant's review of records from MoneyGram, SUBJECT ACCOUNT 1 is also the sender's email address for at least 47 MoneyGram payments from Sanel Smajlovic to various recipients in the Philippines between January 2017 to February 2018.

36. Based on your affiant's review of records from Yahoo and Google, SUBJECT ACCOUNT 1 also closely resembles the recovery email address for the otaku_sanel@sbcglobal.net account. The recovery email address is listed as "sanelsss@gmail.com," which is the SUBJECT ACCOUNT 1 address with the addition of an extra "s." Yahoo Inc (which manages sbcglobal email accounts) reported the recovery email address was input by the user but never verified. In addition, records from Google showed "sanelsss@gmail.com" is not a valid email address on their service. When taken together, these

facts form a strong inference that "sanelsss@gmail.com" was merely a typing error entry for SUBJECT ACCOUNT 1.

37. Your affiant's review of Google subscriber data for SUBJECT ACCOUNT 1 shows it belonging to a subject known simply as "s." However, it has an account recovery phone number set as +13142556957, which T-Mobile records confirmed is subscribed to Sanel SMAJLOVIC at 6942 Colonial Woods Dr Apt 70, Saint Louis, MO 63129.

38. Your affiant reviewed records from PayPal and learned that SUBJECT ACCOUNT 2 is the primary email address listed for PayPal account 1519143165246381427, which is attributed to Sanel SMAJLOVIC. The account was opened March 3, 2018, and shows open status. The account lists additional email addresses of otaku_sanel@sbcglobal.net and SUBJECT ACCOUNT 1. The account also lists the same 314-255-6957 phone number subscribed to Sanel SMAJLOVIC and home address of 6942 Colonial Woods Dr Apt 70, Saint Louis, MO 63129. This PayPal account has four attempted payments to a recipient in the Philippines using PinoyLoads.com. According to their website, "PinoyLoads is known as a swift online loading station, where you can load online and send load to the Philippines with confidence." Your affiant cross-referenced at least one attempted payment through PinoyLoads using this PayPal account, that occurred on or around March 3, 2018, and found it corresponds to the date and time that Skype user "xflinkx" negotiated for live sex show involving a five-year-old girl. In the chat, the trafficker and "xflinkx" discuss various ways to make payment. The user of "xflinkx" acknowledged he is banned from multiple payment platforms. Eventually, "xflinkx" acknowledges that payment through "PinoyLoads" worked, but processing the payment may take extra time as a first-time buyer through the platform.

39. In my training and experience, Sanel SMAJLOVIC's use of multiple accounts on the same payment platform, use of multiple different payment platforms, admission that he is banned from several payment platforms, and use of multiple different email addresses in connection with payment platforms is consistent with the behavior of other known examples of traffickers and customers engaged in international trade of live sex shows or child pornography. Moreover, review of email records known to be linked to this illicit activity is likely to reveal associations with other yet to be identified accounts used for online payment, cloud storage, or online chat and live video.

40. Therefore, Google's servers are likely to contain stored electronic communications and information concerning the user of sanelss@gmail.com and ssbihsss@gmail.com and their use of Google's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

41. On September 13, 2023, a Grand Jury for the Eastern District of Missouri returned a sealed indictment charging SMAJLOVIC with four counts of attempted production of child pornography. (4:23-CR-00490-SRC-RHH). These four counts relate to the investigation outlined above. A sampling of SMAJLOVIC's chat records for each count is as follows:

a. For Count I, the SMAJLOVIC corresponded with a user (hereinafter, "TRAFFICKER 2") over Skype on February 9, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering a five-year-old child and 10-year-old child, and a price is eventually negotiated. During the live stream, the SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "yes do fingering," "put finger in straight I can't see like that," "I want see it go inside hehe," and "show me both girls open pussy." The

live stream ends, and TRAFFICKER 2 confirms that he/she has received the SMAJLOVIC's payment.

b. For Count II, the SMAJLOVIC corresponded with TRAFFICKER 2 on August 17, 2019. SMAJLOVIC is told that TRAFFICKER 2 is offering an 11-year-old child, and a price is eventually negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 2; "ye shes nice cute girl but I like 3-5 more ehe(sic). Even 1-3 sometimes haha," "how deep u can put finger her?", "finger all inside?", "ok hun this time I do for that girl but try find me younger hehe. Or some girl before but more deep? Hehe." When TRAFFICKER 2 tells SMAJLOVIC, "its deep now she getting hurt now," SMAJLOVIC responds, "more deep hun." The live stream ends, and TRAFFICKER 2 confirms that he/she received SMAJLOVIC's payment.

c. For Count III, SMAJLOVIC corresponded with a different user (hereinafter, "TRAFFICKER 3") on October 6, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a one-year-old child. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "and lol what u can do with the 1? Nothing? I think too young for me but can I see? Hehe," "can you open lips more? Hehe," "finger her? Or no?", and "nice hehe." SMAJLOVIC eventually provides TRAFFICKER 3 with payment on October 16, 2018.

d. For Count IV, SMAJLOVIC corresponded with TRAFFICKER 3 on June 23, 2018. SMAJLOVIC is told that TRAFFICKER 3 is offering a six-year-old child and ten-year-old child, and a price is negotiated. During the live stream, SMAJLOVIC makes the following requests/statements to TRAFFICKER 3; "can u wake the 6?", "I like her more," "ye…wake her for show? Or let her sleep u can still show her hehe," and "tell the

10 to put finger in the 6yo pussy hehe." The live stream ends, and TRAFFICKER 3 confirms that he/she has received the SMAJLOVIC's payment.

42. Your affiant's review of the chat logs pertaining to Skype account "xflinkx" revealed this type of activity occurred until at least August 31, 2019. Your affiant's diligent search of available law enforcement databases revealed no intervening law enforcement action that would have stopped SMAJLOVIC from continuing this conduct. In my experience with similar investigations and in consultation with other law enforcement investigating child sex traffickers in the Philippines, it is common for traffickers and customers to change out account usage on various chat applications, including Skype. In fact, in the chat logs from Microsoft I found examples where the user of "xflinkx" references knowing traffickers from their other username or ID or from other chat rooms or platforms.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

44. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time

convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

45. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

46. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.

Nicholas W Zotos

NICHOLAS ZOTOS
Special Agent
Homeland Security Investigations

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 22nd day of September 2023.

Patricia L. Cohen

HONORABLE PATRICIA L. COHEN
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with sanelss@gmail.com and ssbihsss@gmail.com ("the Accounts") that is stored at premises owned, maintained, controlled, or operated by Google LLC and Google Payment Corporation a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google LLC and Google Payment Corporation ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google. Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from April 1, 2017 to Present, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Telephone numbers, including SMS recovery and alternate sign-in numbers;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user

belongs or communicates with; user settings; and all associated logs and change history.

f. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history.

g. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created,

stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun; routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.

k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.

l. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history.

m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.

n. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

o. All records, content, and other information relating to YouTube use and access, including, but not limited to, associated videos (including records of uploads, shares, views, edits, comments, likes, and other interaction; and copies of videos uploaded to, shared by, or shared with the account), searches (including search terms), channels, subscriptions and subscribers, playlists, connected apps, user settings, friends and other contacts (including the content of all communications), deletions and other changes, and, for videos, URL, metadata, privacy and other settings, size, title, description, duration, tags, timestamps, IP addresses, location information, and the account or other identifier of the user who uploaded the video; video and channel performance information, including all analytics on content,

reach, engagement, audience, revenue, and research; and, for all of the above, all related logs, IP addresses, timestamps, and device identifiers.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes contraband, evidence, and instrumentalities of violations of 18 U.S.C. § 2251, 2252A(a)(2), and (a)(5)(B), those violations involving Sanel SMAJLOVIC and occurring from at least as early as April 28, 2017, to Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The production, purchase, receipt, or possession of child pornography or attempts to commit, including any such contraband material stored within Google Drive or as attachments to messages, even when deleted or marked for deletion;

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the Account about matters relating to receipt and distribution of child pornography, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by _____, and my official title is _____. I am a custodian of records for_____. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of _____, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of _____; and

c. such records were made by _____ as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date Signature